

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-150550
(43)Date of publication of application : 23.05.2003

(51)Int.Cl. G06F 15/00
G06F 1/00

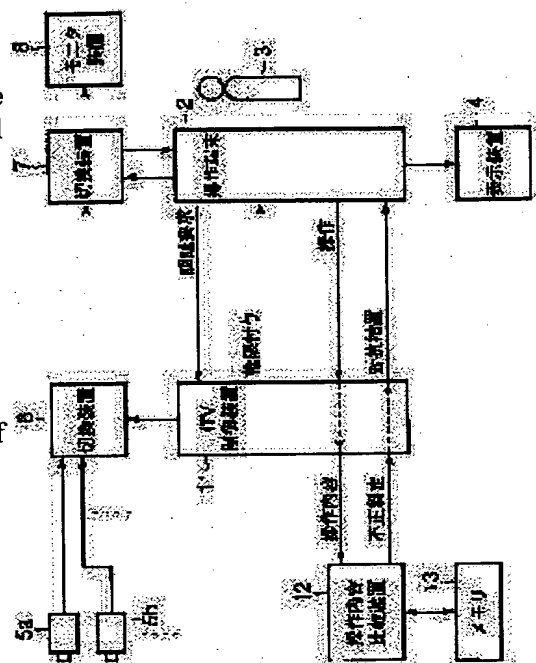
(21)Application number : 2001-349154 (71)Applicant : TOSHIBA CORP
(22)Date of filing : 14.11.2001 (72)Inventor : ENOMOTO HIDEAKI

(54) INFORMATION PROCESSING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the lengthening of the period of an illicit access by successively judging whether or not the operator is a formal operator even after log-on is normally executed by using a formal password.

SOLUTION: An operation content comparing device 12 is connected to an ITV control device 11, and the operation content of a specific period is prestored in a memory 13. The operation content comparing device 12 determines whether or not to be normal operation by comparing the present operation content with the operation content stored in the memory 13 after executing log-on in a system. When it is judged that operation is not the normal operation, a countermeasure is executed by setting an illicit level of 'small', 'medium', and 'large'. A warning is displayed in the level of 'small', and when illicit operation continues further, a level is transferred to the level of 'medium' to display the effect of making illicit access, and log-out is forcibly executed. When the illicit operation continues by executing the log-on again with the same password, the level is transferred to the level of 'large' to forcibly execute the log-out, and an account of the operator 3 is set unusable.



LEGAL STATUS

[Date of request for examination] 18.10.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-150550

(P2003-150550A)

(43) 公開日 平成15年5月23日 (2003.5.23)

| (51) Int.Cl. ⁷ | 識別記号 | F I | テマコード* (参考) |
|---------------------------|-------|---------------|-------------------|
| G 0 6 F 15/00 | 3 3 0 | G 0 6 F 15/00 | 3 3 0 A 5 B 0 8 5 |
| 1/00 | 3 7 0 | 1/00 | 3 7 0 E |

審査請求 未請求 請求項の数 5 O L (全 5 頁)

(21) 出願番号 特願2001-349154 (P2001-349154)

(22) 出願日 平成13年11月14日 (2001.11.14)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 榎本 秀明

東京都港区芝浦一丁目1番1号 株式会社

東芝本社事務所内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

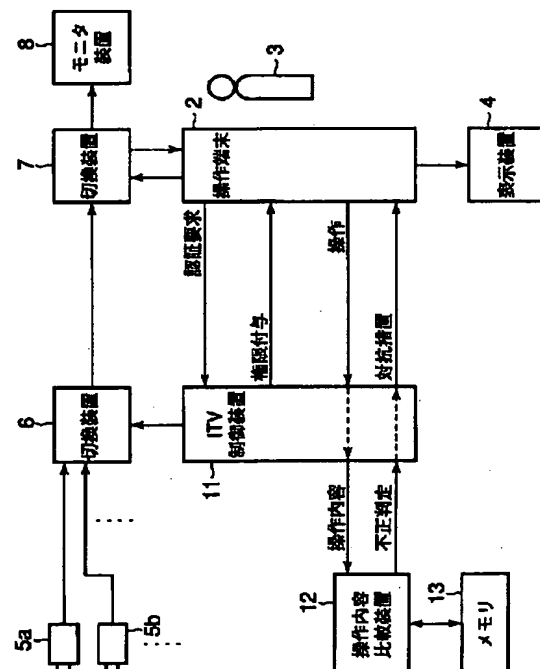
Fターム (参考) 5B085 AE03 AE06 AE15

(54) 【発明の名称】 情報処理システム

(57) 【要約】

【課題】 正式なパスワードを使用して正常にログオンされた後においても、正式な操作者かどうかを逐次判断して不正アクセスの長期化を防止する。

【解決手段】 I T V制御装置 1 1 に操作内容比較装置 1 2 を接続し、メモリ 1 3 に予め一定期間の操作内容を記憶する。操作内容比較装置 1 2 は、システムへのログオンが行なわれた後、現在の操作内容とメモリ 1 3 に記憶している操作内容とを比較して通常操作かどうかを判断する。通常操作ではないと判断された場合、不正レベル「小」、「中」、「大」を設定して対抗措置を実施する。レベル「小」では、警告表示を行ない、更に不正操作が続く場合はレベル「中」に移行し、不正アクセスが行なわれた旨の表示を行なうと共に強制的にログアウトさせる。再度同じパスワードでログオンして不正操作が続く場合、レベル「大」に移行し、強制的にログアウトすると共に操作者 3 のアカウントを使用不可に設定する。



【特許請求の範囲】

【請求項 1】 パスワードを入力して正式な操作者を確認する情報処理システムにおいて、操作アカウント毎に一定期間の操作内容を記憶する記憶手段と、前記操作者による現在の操作と前記記憶手段に記憶されている操作内容とを比較し、現在の操作内容が通常操作と異なる場合に不正操作が行なわれたものと判断する判断手段と、前記判断手段により不正操作が行なわれたものと判断された場合にその操作内容に応じて対抗措置を実施する手段とを具備したことを特徴とする情報処理システム。

【請求項 2】 パスワードを入力して正式な操作者を確認する情報処理システムにおいて、操作アカウント毎に許容する操作内容を予め記憶する記憶手段と、前記操作者による現在の操作と前記記憶手段に記憶されている操作内容とを比較し、現在の操作内容が通常操作と異なる場合に不正操作が行なわれたものと判断する判断手段と、前記判断手段により不正操作が行なわれたものと判断された場合にその操作内容に応じて対抗措置を実施する手段とを具備したことを特徴とする情報処理システム。

【請求項 3】 前記対抗措置を実施する手段は、判断手段により不正操作が行なわれたものと判断された場合にその操作内容に応じて不正レベルを「小」、「中」、「大」に設定し、最初は不正レベル「小」から実施し、不正操作が続けられた場合に順次不正レベル「中」、「大」の対抗措置を実施することを特徴とする請求項 1 又は 2 記載の情報処理システム。

【請求項 4】 前記対抗措置を実施する手段は、判断手段により不正操作が行なわれたものと判断された場合にその操作内容に応じて不正レベルを「小」、「中」、「大」に設定し、不正レベル「小」では操作端末画面上に警告表示を行ない、その後、不正操作が続く場合に不正レベル「中」に移行して操作端末画面上に不正アクセス表示を行なって強制的にログアウトし、更に再度同じパスワードでログオンして不正操作が続けられた場合に不正レベル「大」に移行して強制的にログアウトすると共にその操作者のアカウントを使用不可に設定することを特徴とする請求項 1 又は 2 記載の情報処理システム。

【請求項 5】 前記対抗措置を実施する手段は、判断手段により不正操作が行なわれたものと判断された場合に、その操作内容がシステム上保安性の高い部分に関連する操作かどうかを判断し、保安性の高い部分に関連する操作の場合には最初からレベル「中」あるいはレベル「大」の対抗措置を実施することを特徴とする請求項 3 又は 4 記載の情報処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、端末操作者に対する認証機能を備えた情報処理システムに関する。

【0002】

【従来の技術】従来、例えばプラントの稼働状態や工場の各施設等を監視するシステムとして、図 4 に示すような I TV (industrial television) システムが用いられている。

【0003】図 4 において、1 は I TV 制御装置、2 は上記 I TV 制御装置 1 の操作端末である。この操作端末 2 は、操作者 3 によって操作されるもので、その操作に対応した情報を表示装置 4 に表示する。

【0004】上記 I TV 制御装置 1 は、操作端末 2 の操作に従って監視カメラ 5 a、5 b、…の切換装置 6 を制御する。上記監視カメラ 5 a、5 b、…は、例えばプラントや工場等の監視対象領域に設置される。上記監視カメラ 5 a、5 b、…により撮影された監視画像は、切換装置 6 により選択され、更に切換装置 7 を介してモニタ装置 8 へ送られる。上記切換装置 7 は、操作端末 2 によって切換え制御され、監視画像をモニタ装置 8 へ出力すると共に、操作端末 2 側にも出力できるようになっている。すなわち、操作端末 2 は、モニタ装置 8 に表示される監視画像を切換装置 6 を介して取り込み、自己の表示装置 4 に表示できるようになっている。

【0005】上記のように構成された I TV システムでは、I TV 制御装置 1 に予め操作者 3 に対するパスワードを登録しておき、操作開始時にパスワードの正否を認証するようになっている。すなわち、操作端末 2 は、操作者 3 が操作を開始する際、表示装置 4 にパスワードの入力画面を表示し、操作者 3 がパスワードを入力すると、I TV 制御装置 1 に対してパスワードが正しいかどうかの認証要求を行なう。I TV 制御装置 1 は、入力されたパスワードと予め登録されているパスワードとを比較認証し、正式なパスワードであれば操作端末 2 への操作入力を許可し、操作者 3 に対して操作権限を付与する。

【0006】

【発明が解決しようとする課題】上記従来の I TV システムでは、操作開始時にパスワードの認証処理を行なっているため、正式なパスワードを知らない不正操作者による入力を拒否することができる。

【0007】しかし、従来の I TV システムでは、例えばパスワードを盗まれたり、あるいは不正に解読された場合、それを使ってシステムに正常にログオンされてしまうと、操作者が不正な権限利用を行なっていることを見分けられず、長期間の不正アクセスを許してしまうという問題があった。

【0008】本発明は上記の課題を解決するためになされたもので、正式なパスワードを使用して正常にログオンされた後においても、正式な操作者かどうかを逐次判断して不正アクセスの長期化を防止することができる情報処理システムを提供することを目的とする。

【0009】

【課題を解決するための手段】本発明に係る情報処理シ

システムは、パスワードを入力して正式な操作者を確認する情報処理システムにおいて、操作アカウント毎に一定期間の操作内容を記憶する記憶手段と、前記操作者による現在の操作と前記記憶手段に記憶されている操作内容とを比較し、現在の操作内容が通常操作と異なる場合に不正操作が行なわれたものと判断する判断手段と、前記判断手段により不正操作が行なわれたものと判断された場合にその操作内容に応じて対抗措置を実施する手段とを具備したことを特徴とする。

【0010】上記の構成によれば、正式なパスワードを使用してシステムに正常にログオンした後も、操作者による操作を記憶・分析し、正式な操作者かどうかを逐次判断して不正アクセスに対する対抗措置を実施することができる。従って、正式なパスワードが盗まれたり、不正に解読された場合でも、不正アクセスの長期化を確実に防ぐことができ、システムのセキュリティを向上することができる。

【0011】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態を説明する。図1は、本発明の一実施形態に係るITVシステムの構成を示すブロック図である。図1において、11はITV制御装置、2は上記ITV制御装置11の操作端末である。この操作端末2は、操作者3によって操作されるもので、その操作に対応した情報を表示装置4に表示する。

【0012】上記ITV制御装置11は、操作端末2の操作に従って監視カメラ5a、5b、…の切換装置6を制御する。上記監視カメラ5a、5b、…は、例えばプラントや工場等の監視対象領域に設置される。上記監視カメラ5a、5b、…により撮影された監視画像は、切換装置6により選択され、更に切換装置7を介してモニタ装置8へ送られる。上記切換装置7は、操作端末2によって切換え制御され、監視画像をモニタ装置8へ出力すると共に、操作端末2側にも出力できるようになっている。すなわち、操作端末2は、モニタ装置8に表示される監視画像を切換装置6を介して取り込み、自己の表示装置4に表示できるようになっている。

【0013】上記ITV制御装置11には、予め操作者3に対するパスワードを登録しておき、操作開始時にパスワードの正否を認証し、正式なパスワードであれば操作端末2への操作入力を許可し、操作者3に対して操作権限を付与する機能を備えている。更に、ITV制御装置11には、操作内容比較装置12が接続される。この操作内容比較装置12は、各アカウント毎の操作内容を記憶するためのメモリ13を備えている。上記操作内容比較装置12は、操作アカウント毎に一定期間の操作内容をメモリ13に記憶し、それを基準にして現在の操作内容と比較することにより不正アクセスを検出してITV制御装置11へ出力する。ITV制御装置11は、操作内容比較装置12により不正アクセスが検出された場

合、その程度に応じて不正レベル「小」、「中」、「大」を設定すると共に、例えば「不正表示」、「ログアウト」、「アカウント使用不可」等の対抗措置を実施する。

【0014】次に、上記実施形態における不正アクセスの検出動作を図2及び図3に示すフローチャートを参照して説明する。図2は、操作開始時のパスワード入力に対する処理動作を示すフローチャートである。操作者3は、操作を開始する際、操作端末2よりパスワードを入力する(ステップA1)。操作端末2は、パスワードが入力されたことを検知すると(ステップA2)、ITV制御装置11に対して認証要求を行なう。ITV制御装置11は、上記認証要求により認証処理を開始し(ステップA3)、入力されたパスワードと予め登録されているパスワードとを比較し、入力されたパスワードが正式のものであるか否かを判断する(ステップA4)。入力されたパスワードが間違っていれば、その旨を表示装置4に表示して再度の入力に備える。また、入力されたパスワードが正しい場合には、ITV制御装置11から操作端末2へ操作権限を付与する情報を操作端末2へ送り、その後の操作入力を受付ける(ステップA5)。

【0015】上記のように正常にログオンした場合、その後の操作者3による操作端末2の操作内容、例えば普段どの映像を見るか、どの制御を行なうか、よく使用するボタンはどれか等について、操作アカウント毎に一定の期間例えば1ヶ月の間、ITV制御装置11から操作内容比較装置12へ送ってメモリ13に記憶する。

【0016】次に、上記操作権限が操作者3に与えられた後の処理動作を図3に示すフローチャートに従って説明する。上記のように操作者3の通常の操作内容を操作内容比較装置12のメモリ13に記憶した後、操作者3が操作端末2を操作すると(ステップB1)、その操作内容はITV制御装置11から操作内容比較装置12へ送られる。操作内容比較装置12は、操作者3の操作内容を予めメモリ13に記憶している操作内容と操作アカウント毎に比較し、通常行なわれている操作かどうかを判断し(ステップB2)、その判断結果をITV制御装置11に通知する。上記操作内容比較装置12において、現在の操作が通常操作であると判断された場合、ITV制御装置11は、その操作内容に対応した処理を実行し(ステップB3)、ステップB1に戻って次の入力に備える。

【0017】また、操作内容比較装置12において、現在の操作が通常行なわれていない、あるいは操作者3の職務から外れるようなものであると判断された場合、ITV制御装置11は、その不正レベルに応じた対抗措置を実施する。

【0018】先ず、その操作がシステム上保安性の高い部分に関連する操作かどうかを判断し(ステップB4)、保安性の高い部分に関連する操作でなければ不正

レベルが「小」に設定されているかどうか(ステップB5)、更には「中」に設定されているかどうかを判断する(ステップB6)。不正レベルが「小」、「中」の何れにも設定されていなければ、不正レベルを「小」に設定し(ステップB7)、操作ミスか機器の誤動作である可能性も考慮して、操作端末2の表示装置4に例えば「誤った操作が行なわれましたので、注意して下さい。」等の警告を表示する(ステップB8)。その後、ステップB1に戻って次の入力操作に備える。

【0019】また、上記ステップB5において、既に不正レベル「小」が設定されていると判断された場合、すなわち、上記ステップB7で不正レベル「小」が設定された後、更に不正と思われる操作が続く場合には、ステップB5からステップB9に進んで不正レベルを「中」に設定し、表示装置4に例えば「不正な操作が行なわれました。」等の不正表示を行ない(ステップB10)、強制的にログアウトさせる(ステップB11)。

【0020】また、上記ステップB6において、既に不正レベル「中」が設定されていると判断された場合、すなわち、上記ステップB9で不正レベルが「中」に設定されて強制的にログアウトされた後、再度同じパスワードでログオンして不正と思われる操作が続く場合には、ステップB6からステップB12に進んで不正レベルを「大」に設定し、強制的にログアウトさせる(ステップB13)。更に、その操作者のアカウントを使用不可に設定し(ステップB14)、処理を終了する。

【0021】また、上記ステップB4において、入力操作がシステム上保安性の高い部分に関連する操作であると判断された場合には、直ちにステップB12に進み、最初から不正レベル「大」の措置を実施する。なお、上記ステップB4において、入力操作がシステム上保安性の高い部分に関連する操作であると判断された場合、ステップB9に進んで不正レベル「中」の措置を実施するようにしてもよい。

【0022】上記実施形態に示すように正常にログオンした後も、操作者3による操作を記憶・分析し、正式な操作者かどうかを逐次判断し、不正アクセスに対する対抗措置を実施するようにしたので、正式なパスワードが盗まれたり、不正に解読された場合でも、不正アクセスの長期化を防ぐことができ、システムのセキュリティを向上することができる。

【0023】なお、上記実施形態では、操作者3の一定期間の操作内容をメモリ13に記憶するようにしたが、その他、例えば通常行なう操作内容を予め特定してメモ

リ13に記憶するようにしてもよい。すなわち、操作者3の操作内容は、システムの構成あるいは各操作者の職務等によって特定することができるので、予め許容できる範囲の操作内容をメモリ13に記憶させることが可能である。

【0024】また、上記実施形態では、ITV制御装置11に対して操作内容比較装置12を外部接続する場合について示したが、ITV制御装置11の内部に操作内容比較装置12及びメモリ13を設けても良いことは勿論である。

【0025】また、上記実施形態では、ITVシステムに実施した場合について示したが、その他のシステムであっても、パスワードを使用して正式な操作者を確認する情報処理システムにおいて実施し得るものである。

【0026】

【発明の効果】以上詳記したように本発明によれば、パスワードを使用して正式な操作者を確認する情報処理システムにおいて、システムに正常にログオンした後も、操作者による操作を記憶・分析し、正式な操作者かどうかを逐次判断し、不正アクセスに対する対抗措置を実施するようにしたので、正式なパスワードが盗まれたり、不正に解読された場合でも、不正アクセスの長期化を防ぐことができ、システムのセキュリティを向上することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るITVシステムの構成を示すブロック図。

【図2】同実施形態における操作開始時のパスワード入力に対する処理動作を示すフローチャート。

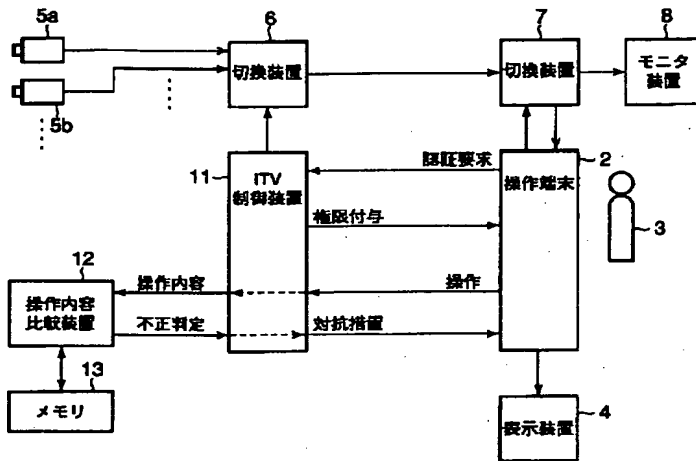
【図3】同実施形態において、正常にログオンした後の不正アクセスに対する処理動作を示すフローチャート。

【図4】従来のITVシステムの構成を示すブロック図。

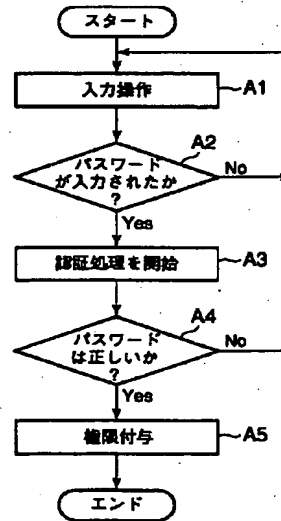
【符号の説明】

- 2…操作端末
- 3…操作者
- 4…表示装置
- 5a、5b、…、…監視カメラ
- 6、7…切換装置
- 8…モニタ装置
- 11…ITV制御装置
- 12…操作内容比較装置
- 13…メモリ

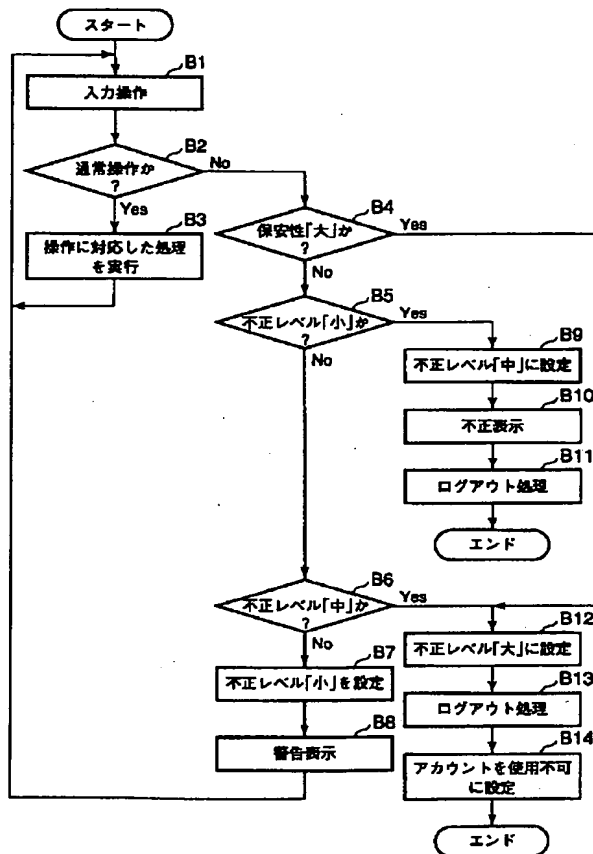
【図1】



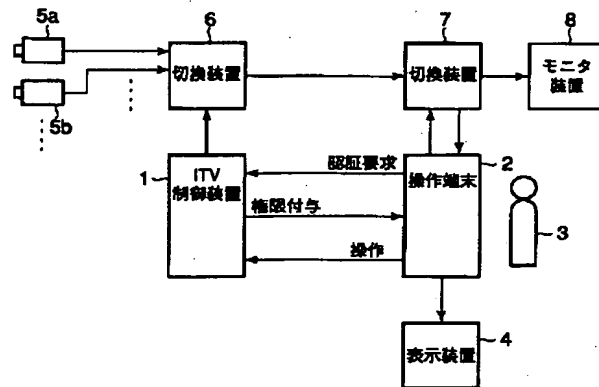
【図2】



【図3】



【図4】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.